Ashore AT/FP Vision Brief

Working Class

June 2005

In the Past. . .

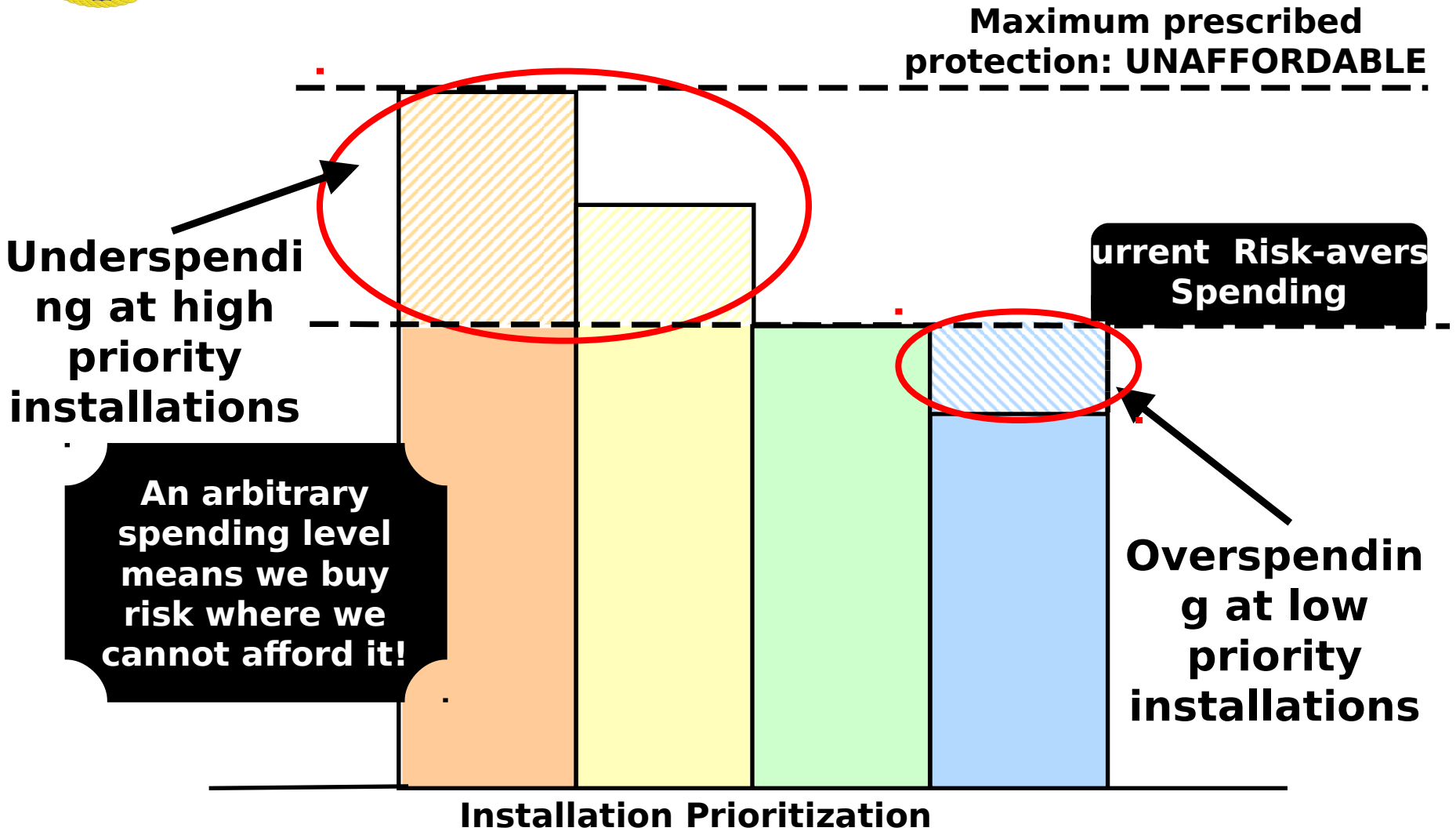
- Navy lacked a single overarching Ashore AT/FP vision
- Efforts were installation-centric with no strategy
- Khobar Towers, USS Cole, and 9/11 drove diffusion and divergence of resource application and readiness output
- Attempted to be everywhere, all the time

RISK AVERSION has been the approach

Inconsistency + No Standardization + Unrealistic Resourcing + Prohibitive cost =

UNATTAINABLE READINESS

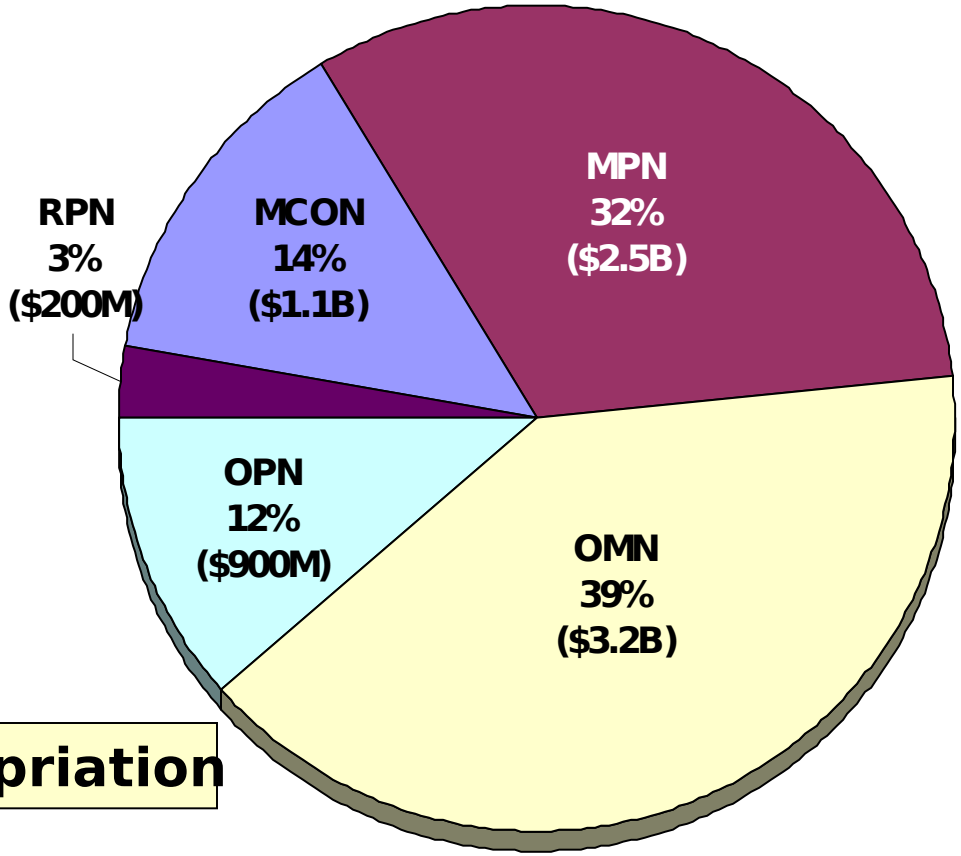
Risk-averse Spending
(Notional)


Maximum prescribed protection: UNAFFORDABLE
Underspending at high priority installations
urrent Risk-avers Spending
An arbitrary spending level means we buy risk where we cannot afford it!
Overspending at low priority installations
Installation Prioritization

Influences

- *GAO Report, "DOD Efforts to Improve Installation Preparedness Can Be Enhanced with Clarified Responsibilities and Comprehensive Planning"* August 2004
  - Recommends Department of Defense incorporates results-oriented management principles and clarifies installation preparedness related responsibilities
- *CJCSI 3170.01D Joint Capabilities Integration and Development Systems (JCIDS)*, 12 March 2004
  - Establishes process to identify, assess, and prioritize joint military capability needs
- *Defense Planning Guidance* (FY2004-2009)
  - Adopt a capabilities based approach to focus on the broad set of capabilities needed to deter, deny and defeat attacks
- *GAO Report, "Combating Terrorism:Actions Needed to Guide Services' Antiterrorism Efforts at Installations"* November 2002
  - Use assessments of threat, vulnerability, and criticality of assets to form foundation of installation antiterrorism plans and support a risk management approach to resource allocation
- *Memorandum from Secretary Wolfowitz*, 5 September 2002
  - Policy of the Department is to protect personnel from CBRNE attacks, to respond to these attacks, and to ensure installations are able to continue critical operations and resume essential operations

Ashore Combating Terrorism Resource



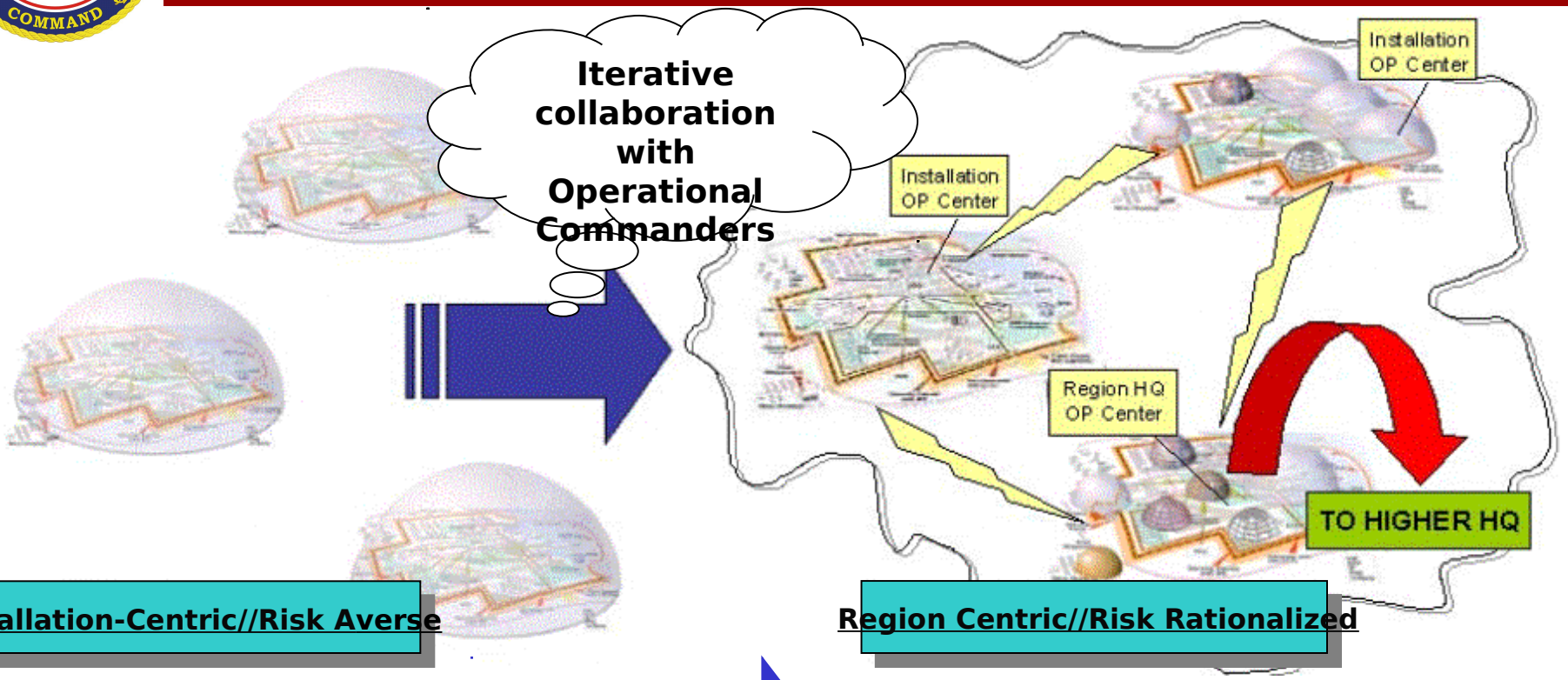
Total = $7.9B
(FY05-09)

Appropriation

CNI's Vision for Implementing AT/FP at Shore Installations

- **Formalized Framework**
- **Region Centric**
- **Capabilities Based**
- **Risk Management Approach**

Now. . .Future



Installation-Centric//Risk Averse

- Aversion to risk – Unachievable
- Slow implementation, increased costs
- Prohibitive cost
- Unrealistic resourcing
- DoD/Joint Vision
- Lack of sustainment

Region Centric//Risk Rationalized

- Management of risk
- Quicker implementation
- Balanced resource application based on Navy-wide capability gaps, criticality, vulnerability, threat
- Formalized framework

Strategy

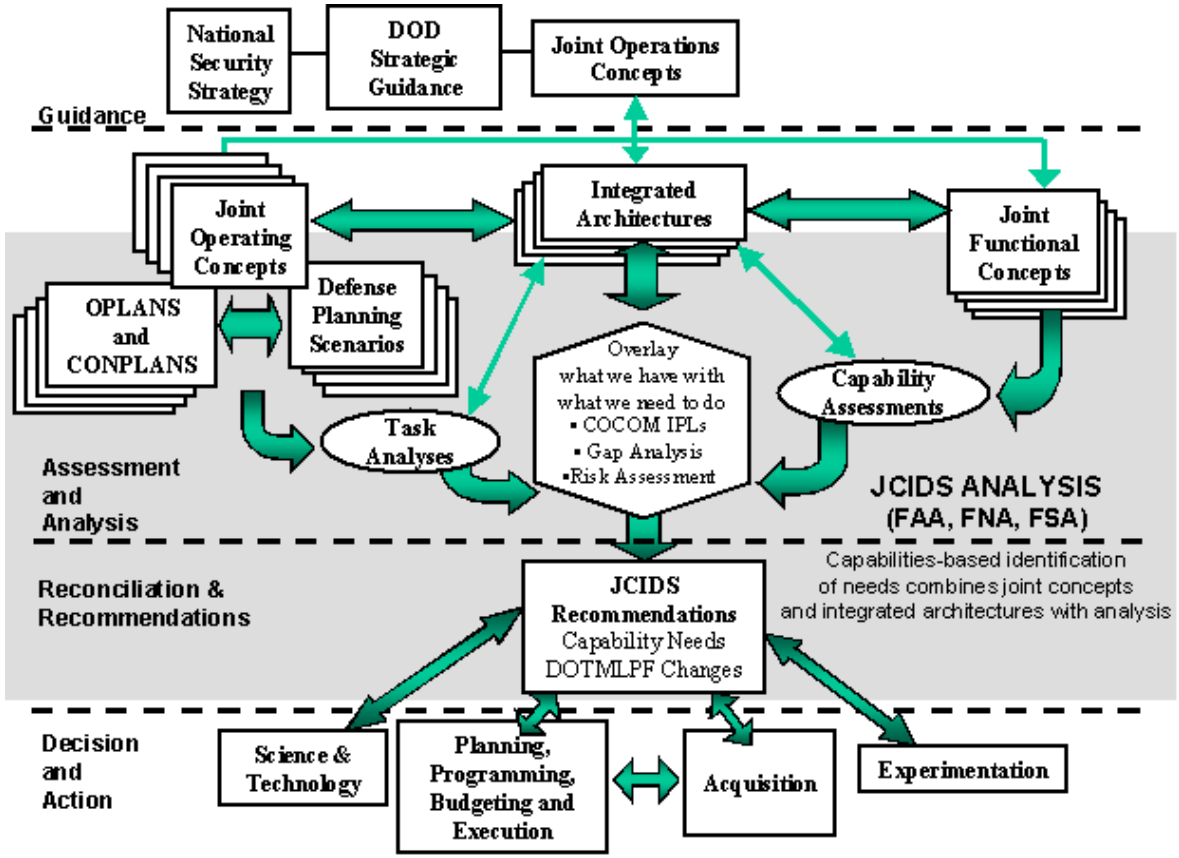
- **Align programs using Joint and General Accounting Office (GAO) guidance**
- **Senior Steering Group (SSG)/SYSCOM Antiterrorism Team (SAT) Process**
  - **Requirements Generation**
  - **Resource/Programming**
  - **Execution**
  - **FFC Advisory Role**
- **Refine FFC/CNI Requirements Identification Process**
- **Fully Realize Public Safety Shore Installation Model starting with Pilot Program development and execution**
- **Implement Risk-Based Investment Strategy**
- **Develop Region-Centric Programs of Record to include sustainment**

Development of Ashore AT/FP Program Process

Basic Tenets

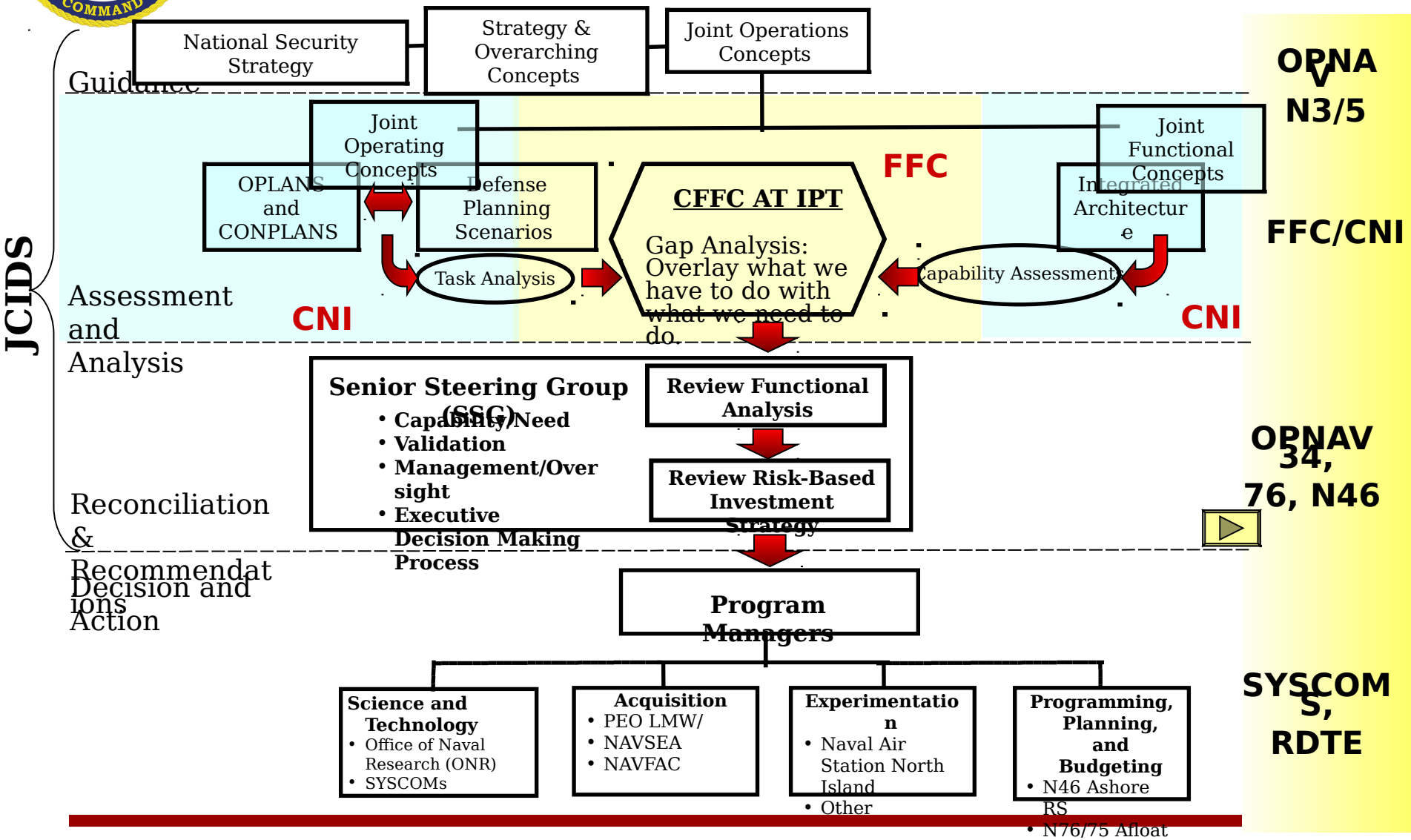
- **Joint Capabilities Integration Development System (JCIDS)**
  - **Joint concept centric capability identification process**
  - **Assess existing and proposed capabilities**
  - **Deliver technologically sound sustainable and affordable increments of capability**
  - **Aligns AT Ashore with the JS Protection FCB**

JCIDS Analysis

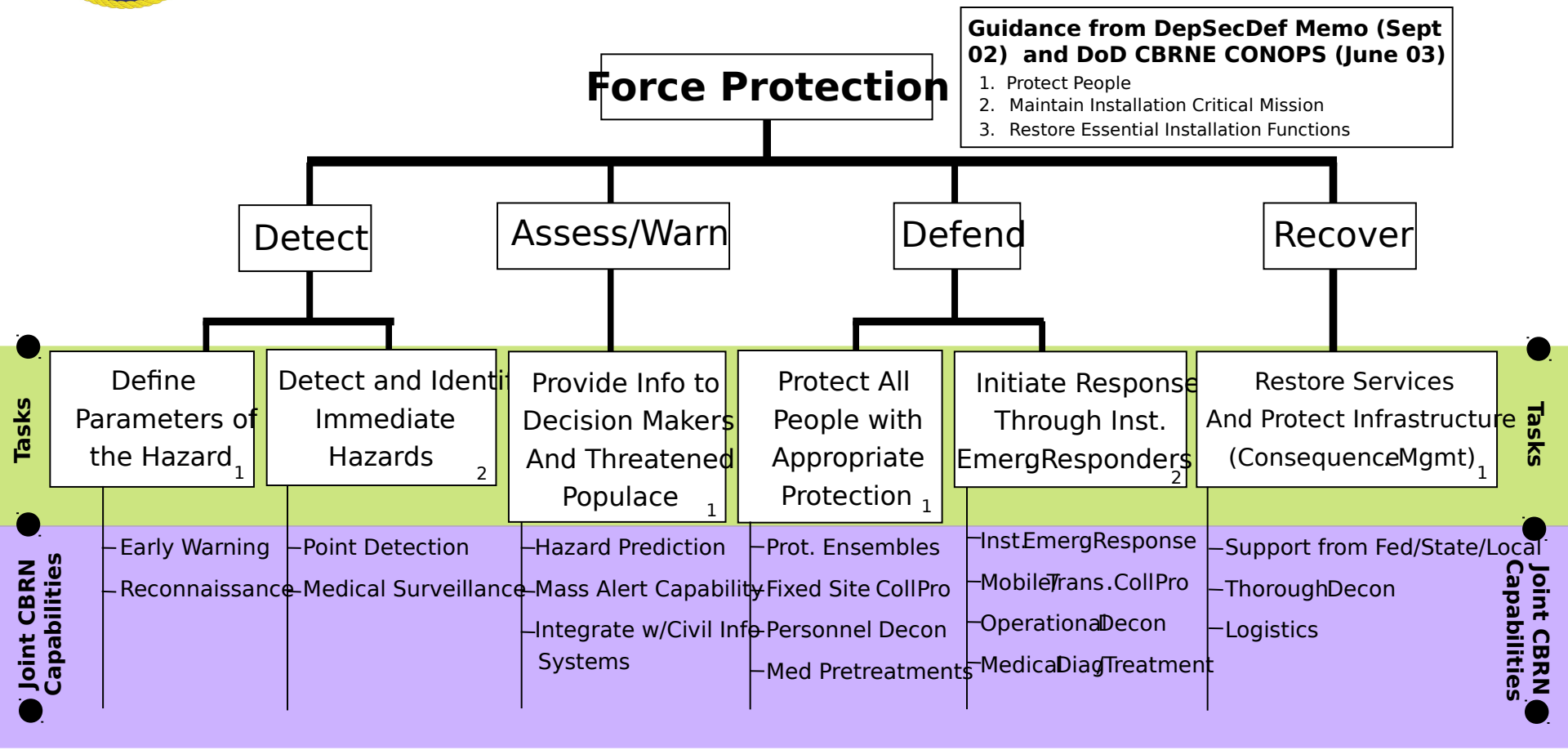


- A capabilities-based approach that leverages government agencies, industries, and academia
- Allows flexibility in meeting security challenges
- Considers the most effective joint force capabilities and integrates them early in the acquisition process

AT/FP Capabilities & Integration Process



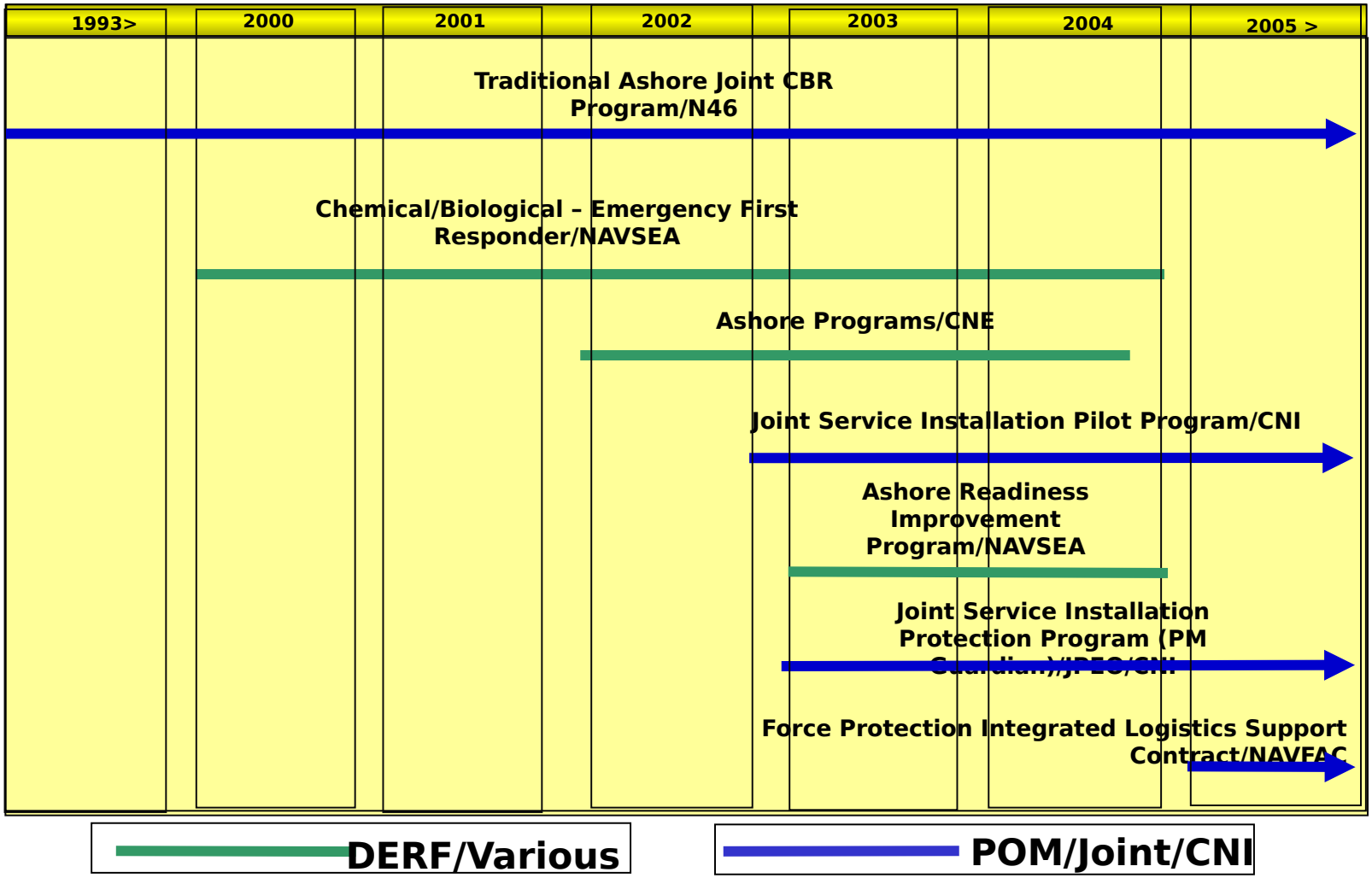
DoD Proposed Ashore AT/FP Architecture



Current Joint/Navy Legacy CBRN Programs

- **Six separate fielding programs**
  - Traditional Ashore Joint CBR Program
  - Chemical/Biological – Emergency First Responder
  - Ashore Programs
  - Ashore Readiness Improvement Program
  - Joint Service Installation Pilot Program
  - Joint Service Installation Protection Program (PM Guardian)
- **One logistics program**
  - Integrated Logistics Support Contract

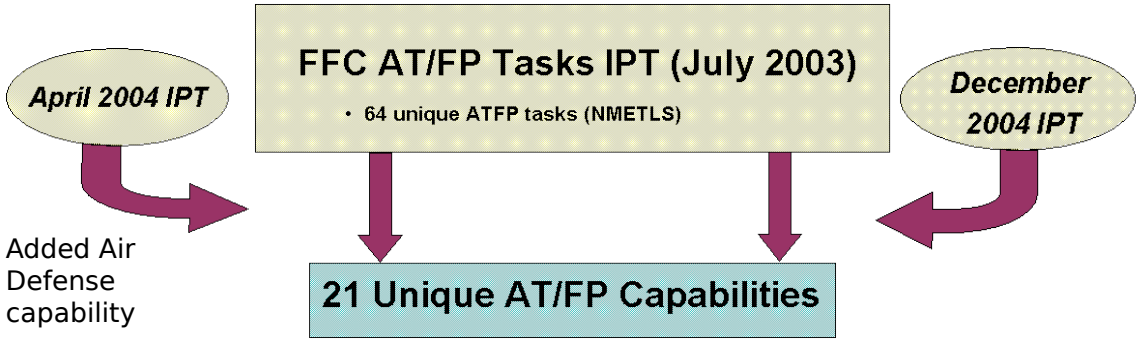
CBRN Programs



CNI Public Safety Strategy for Joint Programs

- **Satisfy Joint Staff Guidance** — Y
- **Align with CB Ashore programs** — G
- **Establish Life Cycle Management** — Y
- **Sustainable and Standardized** — G
- **Assess/quantify impacts of all CBRN equipment being delivered through joint programs (“The Purple Band”) to Regions/Installations to define/de-conflict requirements for Risk Rationalized AT/FP Plan (“The Blue Band”)** — G

CFFC Program Guidance/Priority

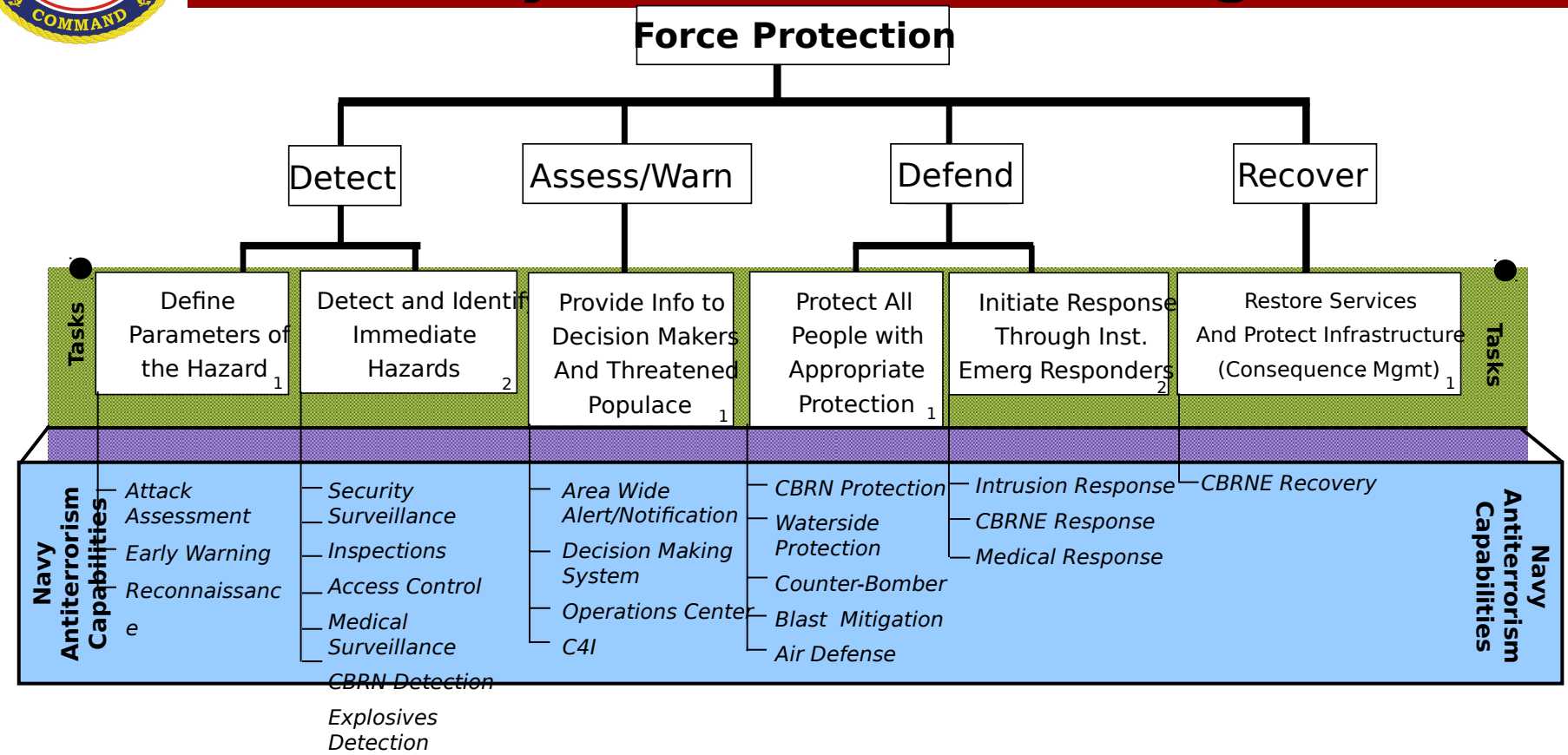

April 2004 IPT
FFC AT/FP Tasks IPT (July 2003)
• 64 unique ATFP tasks (NMETLS)
December 2004 IPT
Added Air Defense capability
21 Unique AT/FP Capabilities

Development and Implementation of Ashore AT/FP Program

"CFFC (4-Star) Intent"

- **Establish and Optimize Cost Effective AT Capabilities**
- **Manage CBRN Expenditures in Support of Joint Programs**
- **Pursue Capability Pilot Projects for Implementation**
  - **Information Management & Base-Wide Alert**
  - **Physical Security/Access Control**
- **Identify Full-Spectrum Capabilities to Facilitate Training, Exercise, and Reporting Requirements**
- **Align AT/FP Capabilities around FFC Requirements IPT Process**

Development and Implementation of Navy Ashore AT/FP Program



The operational tasks identified in the JCIDS analysis define what installations are required to do; capabilities are born from the strategic bundling of unified tasks

Development of CNI Risked-Based Model

ASSERTION

Risk can be analyzed and managed by focusing on Threat, Vulnerability and Criticality

Threat (Likelihood of something bad happening)

–What threats exist today and what is the relative likelihood of each threat?

–How would the likelihood of the threat change by investing in specific antiterrorism capabilities?

Vulnerability (Likelihood controls in place will fail)

–If an attack were attempted, what is the likelihood that it is successful?

–By implementing a specific Force Protection capability, what level of reduction in vulnerability to an attack of this type can be expected?

Criticality (Magnitude of the loss)

–If an attack occurs and is successful, what are the consequences to:

- People
- Assets and Infrastructure
- Mission Capability

DEPSECDEF memo dtd 5 Sept 2002

–By implementing the specific Force Protection capability, what level of reduction in criticality can be expected?

Joint Publication 1-02, 12 April 2001 and GAO Report *"Further Actions Needed to Coordinate Federal Agencies' Facility Protection Efforts and Promote Key Practices"* November 2004

CNI Risk-Based Model

Fleets with CNI Threats (MTAC)

CVAMP Vulnerabilities

Criticalities

Capabilities

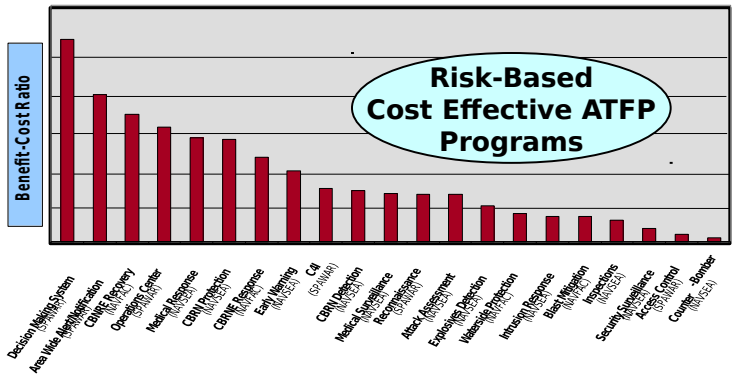
SYSCOM AT/FP PMs

Technology Maturity

Deployability

Threat type	Target	Criticality: People	Criticality: Economic	Criticality: Mission	Baseline	Risk Impact of AT Capability: Attack Assessment	Early Warning	Reconnaissance	Security Surveillanc	Inspections	Access Control	Medical Surveillanc	CBRN Detection	Explosives Detectio	Area Wide Alert/Notification	Decision Making Sy
Land	Personnel															
	Relative Threat:															
	Vulnerability:															
	Criticality:															
Land	Structures															
	Relative Threat:															
	Vulnerability:															
	Criticality:															
Land	Vessels and aircraft															
	Relative Threat:															
	Vulnerability:															
	Criticality:															
Land	CIP															
	Relative Threat:															
	Vulnerability:															
	Criticality:															
Sea	Personnel															
	Relative Threat:															
	Vulnerability:															
	Criticality:															

Conducted risk assessments of potential attack scenarios to assess the effectiveness of AT capabilities defined by JCIDS



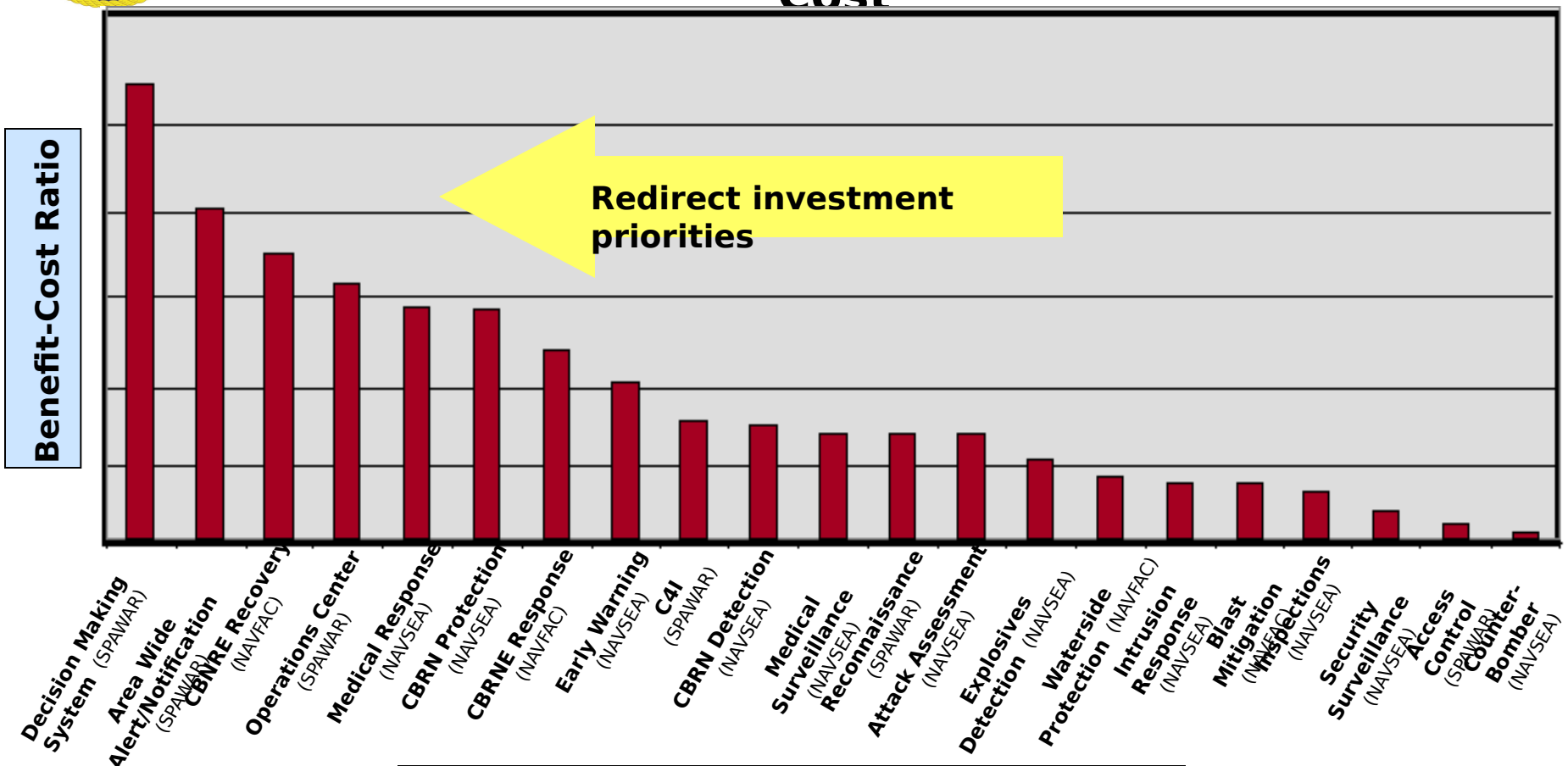
$$= \frac{\left\{\left[\text{Risk}(T/V/C)_{\text{Baseline}}\right] - \left[\text{Risk}(T/V/C)_{\text{WithAT Capability}}\right]\right\} \times (TF) \times (DF)}{\text{Navy Cost of the AT Capability}}$$

Risk(T/V/C) = Risk measured as a function of Threat, Vulnerability, and Criticality
TF = Technology maturity factor
DF = Deployability factor

Published in *The Journal of Homeland Security*, February 2004

CNI Risk-Based Model

AT/FP Capabilities Relative Ranking of Benefit-Cost



Marginal utility curve identifies capabilities that reduce overall FP risk at lower cost

Capability Area Coordinators (CACs) & CA System Engineers (CASEs)

Command & Control CASE: Don Johnson
SPAWAR SSC CH
(858) 537-8698
henry.johnson@navy.mil

Physical Security CASE: Andy Varnava
NFESC
(805) 982-1589
andrew.varnava@navy.mil

CBRN & Medical CASE: Dave Krejdovsky
NSWCDD
(540) 653-2136
david.krejdovsky@navy.mil

Attack Assessment
Kevin Boner / SPAWAR SSC-SD
(619) 553-3558
kevin.boner@navy.mil
D T

Reconnaissance / Detection
John Mitchell / SPAWAR SSC SD
(619) 524-2080
john.w.mitchell@navy.mil
D T

Decision Making System
Philip Bailey / SPAWAR SSC CH
(843) 218-5565
philip.bailey@navy.mil
A

Wide Area Alert/Notify
Tom Charters / SPAWAR SSC SD (619) 553-4864
tom.charters@navy.mil
A

Early Warning
Frank Mazzone / SPAWAR SSC CH
(843) 218-5411
frank.mazzone@navy.mil
D T

Operations Center
Jonathan Searight / SPAWAR SSC CH
(843) 218-4627
jonathan.searight@navy.mil
A

C4I
Kevin Boner / SPAWAR SSC-SD
(619) 553-3558
kevin.boner@navy.mil
A

Access Control
Tom Whittle / SPAWAR SSC CH (215) 847-3104
tom.whittle@navy.mil
D T

Explosives Detection
Mike Troffer / EODTECHDIV
(301) 744-6850 x 269
trofferma@eodpoe2.navsea.navy.mil
D T

Air Defense
Brandy Flotten / NAVAIR
(773) 324-7237
brandy.flotten@navy.mil
D F

Inspections
Jeremy Flamion / NSWC Crane
(812) 854-4790
jeremy.flamion@navy.mil
D T

Intrusion Response
Dawn Hoffa / NSWC Crane
(812) 854-4790
dawn.hoffa@navy.mil
D F

Waterside Protection
Bob Taylor / NFESC
(805) 982-5914
robert.taylor5@navy.mil
D F

Security Surveillance
Edmund Doray / NSWCDD
(850) 235-5079
edmund.doray@navy.mil
D T

Counter-Bomber
Mike Troffer / EODTECHDIV
(301) 744-6850 x 269
trofferma@eodpoe2.navsea.navy.mil
D F

Blast Mitigation
Jim Tancreto / NFESC
(805) 982-1180
james.tancreto@navy.mil
D F

Medical Surveillance
Dave Krejdovsky / NSWCDD
(540) 653-2136
david.krejdovsky@navy.mil
D T

Medical Response
Duane Caneva / MC USNR (202) 762-0299
dccaneva@us.med.navy.mil
D F

CBRNE Response
Pete Novick / NAVFAC HQ
(202) 685-9352
peter.novick@navy.mil
D F

CBRN Detection
Dave Krejdovsky / NSWCDD
(540) 653-2136
david.krejdovsky@navy.mil
D T

CBRN Protection
Dave Krejdovsky / NSWCDD
(540) 653-2136
david.krejdovsky@navy.mil
D F

CBRN Recovery
Pete Novick / NAVFAC HQ
(202) 685-9352
peter.novick@navy.mil
R

D T — Detect
A — Assess/Warn
D F — Defend
R — Recover

SPAWAR
NAVSEA (non-CBR)
NAVSEA (CBR)
NAVFAC
NAVAIR

AT/FP ASHORE PM
Darrell Kim
NAVFAC
(202) 685-9334
darrell.kim@navy.mil

Required Operational Capabilities (ROC) Construct

ROC 1- <u>Strategic Asset & High Threat Bases</u> (2%)*

(a) Provides protection for nuclear weapons and supporting systems (SSBNs). Staffed to support current DoD (41M) security requirements.

(b) Requires special protection requirements due to their high threat environment. Tailored staffing to support fulltime C/D.

ROC 2 - <u>Operational Bases (OB) and critical C4ISR</u> (40%)

- Major fleet homeports home-ported combatant ships and/or tactical aircraft; forward operating locations (OCONUS); critical load-out/ embarkation stations; and critical C4ISR communication stations.

ROC 3 - <u>Sustainment & Support Activities (S&SA)</u> (33%)

(a) Sustainment - Hospitals, bases with non-combatant ships, non-tactical aircraft, weapons storage facilities, logistics sites, shipyards & maintenance facilities.

(b) Support - headquarters, and communication sites; and includes any enclave area associated with ROC 2 bases.

ROC 4 - <u>Administrative and Training Activities (A&TA)</u> (25%)

- Reserve bases; R&D centers; administrative facilities/complexes, i.e. BUPERS Millington; recreational areas and MWR facilities; exchanges and commissaries; training sites, e.g. Naval Academy and Staff Colleges; museums and displays like the USS Constitution; and includes any enclave area associated with ROC 2 or 3 bases.

*Percentage of Navy installations

NMET Conditions and Measures

NTA: Establish and Enforce Protection Perimeter

Supported Capability: Access Control

Conditions: CONUS/OCONUS, ashore, afloat, All Weather

Measures:

M1 Yes/No – Force Protection Perimeter established IAW ATFP plan? Scalable from CL1-4

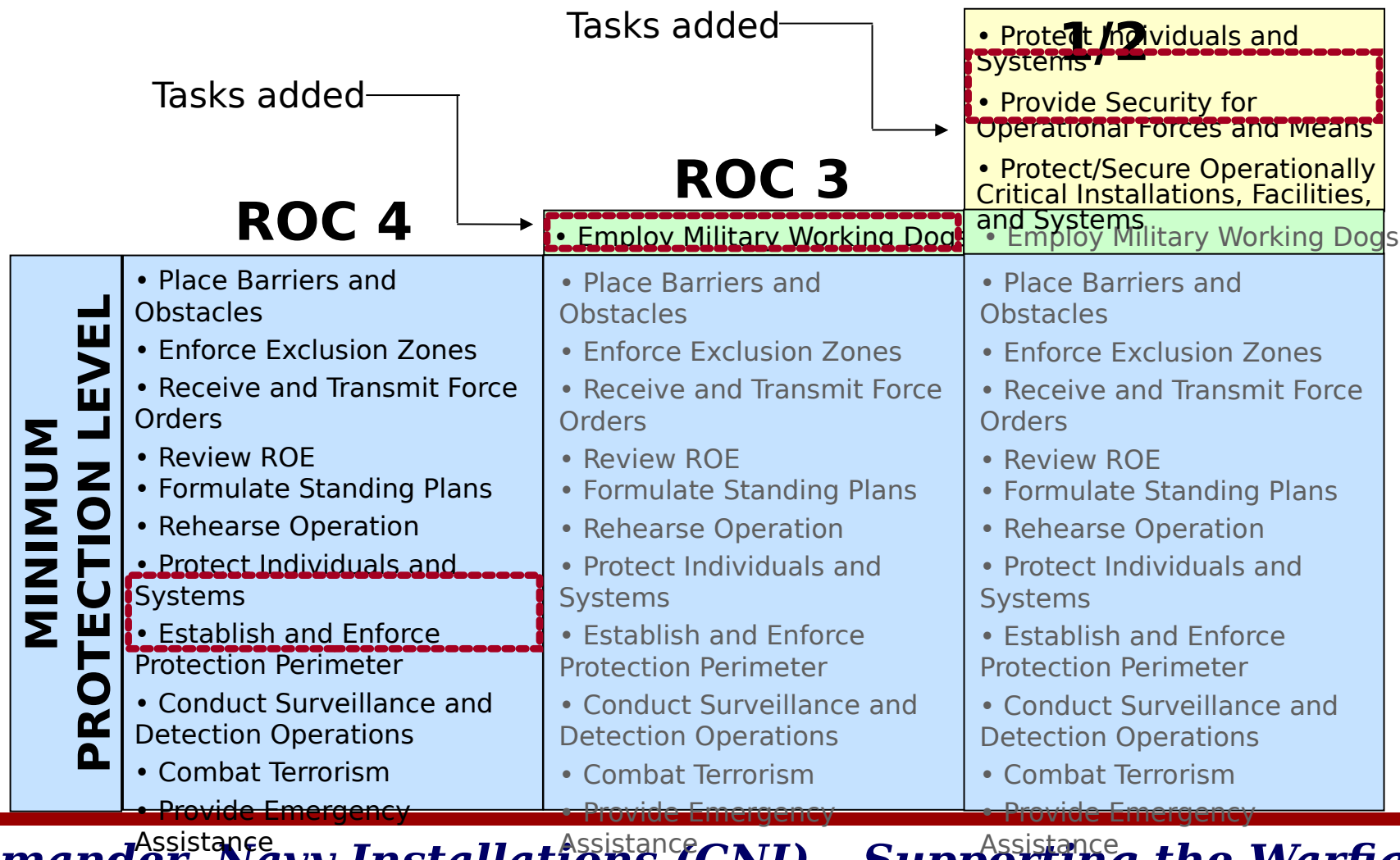
M2 Percent – Perimeter penetrations repelled. Scalable from CL1-4

NMETS are the basis of metrics for:

- Material resourcing
- Manpower resourcing
- Readiness tracking
- Training standards for unit exercises
- DOTMLPF

Fleet Forces Command website, Antiterrorism (AT) Library

NMET Scalability ROC – Access Control


ROC 4
ROC 3
ROC 1/2
Tasks added
Tasks added
MINIMUM PROTECTION LEVEL
• Place Barriers and Obstacles
• Enforce Exclusion Zones
• Receive and Transmit Force Orders
• Review ROE
• Formulate Standing Plans
• Rehearse Operation
• Protect Individuals and Systems
• Establish and Enforce Protection Perimeter
• Conduct Surveillance and Detection Operations
• Combat Terrorism
• Provide Emergency Assistance
• Employ Military Working Dogs
• Protect Individuals and Systems
• Provide Security for Operational Forces and Means
• Protect/Secure Operationally Critical Installations, Facilities, and Systems

NMET Scalability
ROC – Access Control Sample

Perimeter

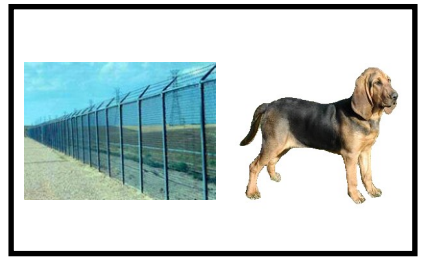
Military Working Dogs

Security Technology

ROC 1

ROC 2

ROC 3



ROC 4

Linking ROCs and CLs

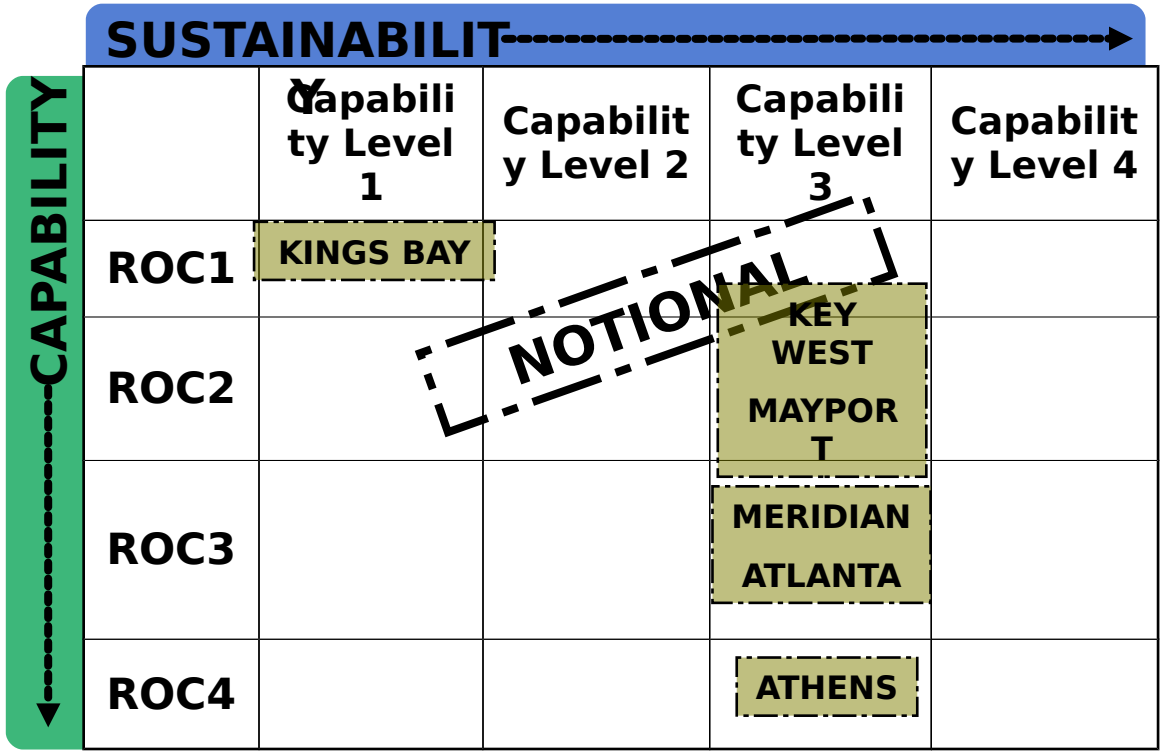
with Notional Regional Overlay

OBJECTIVES

- Better linking of resources to output
- Enhances costing at various levels of performance
- Improves linkage between mission requirements, known capabilities, and performance
- Better aligns product and service delivery with warfighter/customer expectations
- A better assessment of capability versus requirement supporting management of risk.

$$\text{Productivity} \equiv \frac{\text{Output}}{\text{Cost}}$$

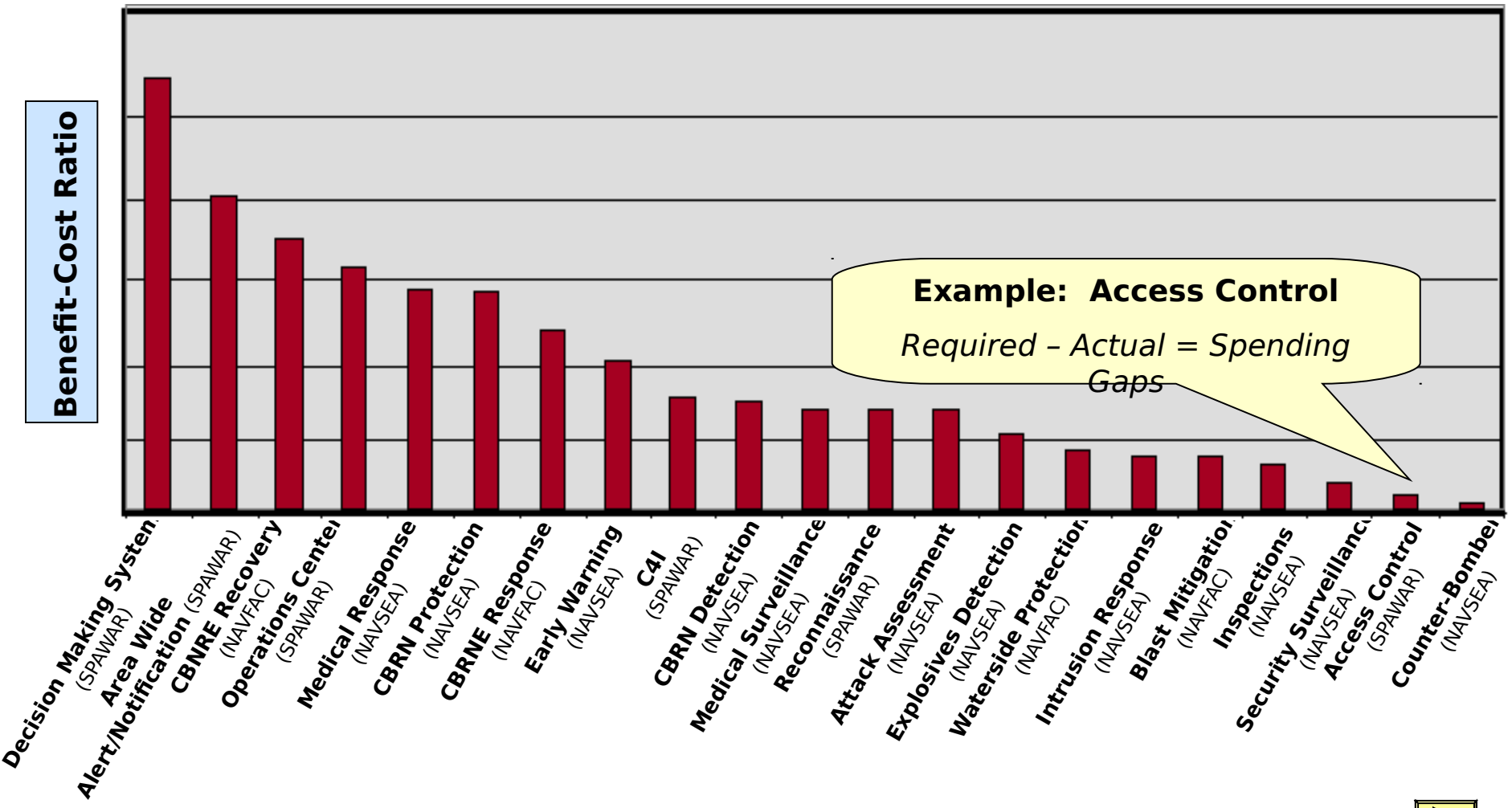
The 4X4 Matrix



Joint Staff Installation & Facility Preparedness Guidance (2004)

CNI Risk-Based Model

AT/FP Capabilities Relative Ranking of Benefit-Cost



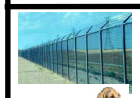
Capability Package (Required)

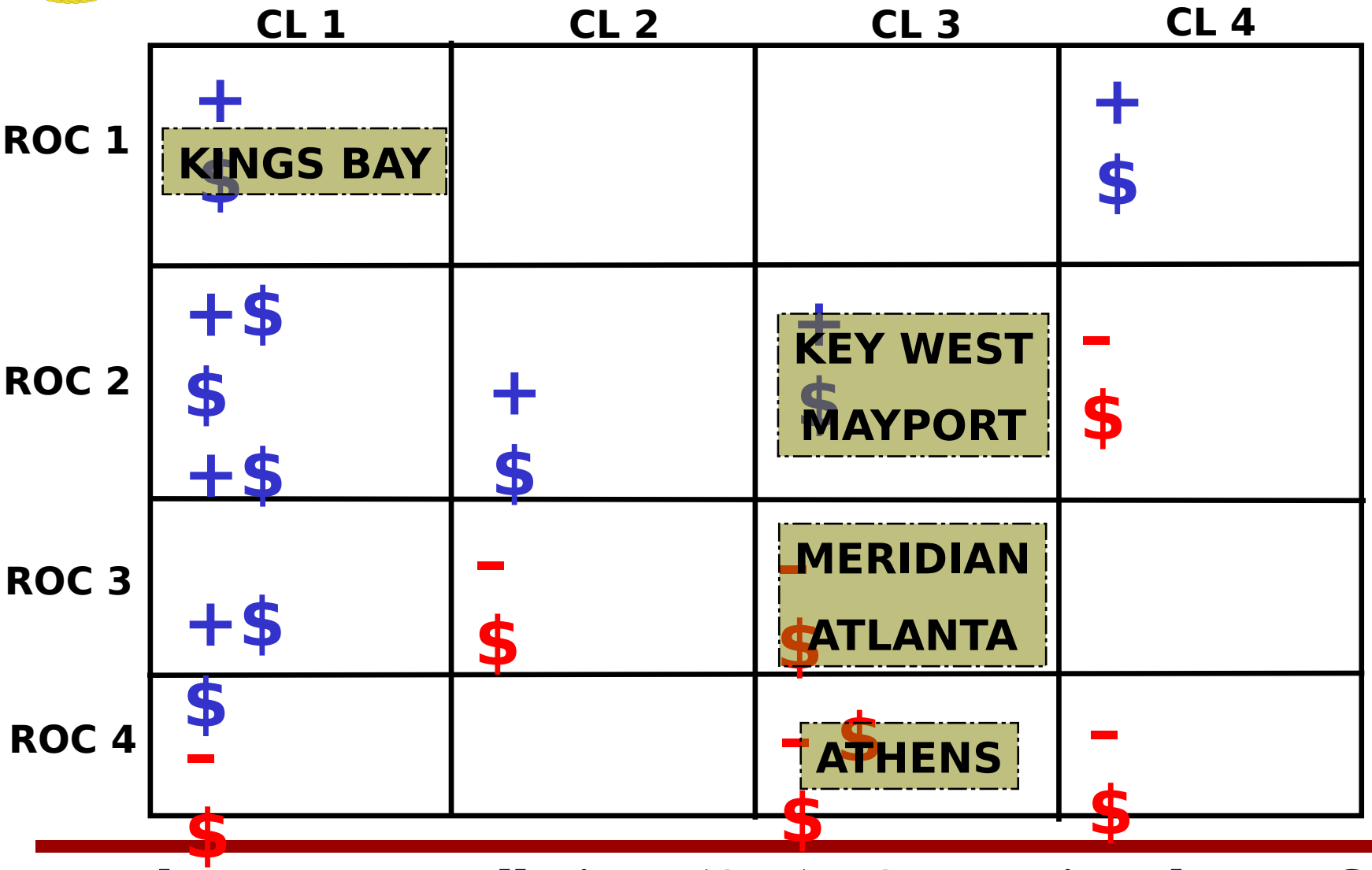
Notional Access Control Sample

	CL 1	CL 2	CL 3	CL 4
ROC 1	Immediate Daily Immediate	Weekly 3 times/week Twice a week	Monthly Once a week Weekly	When available Twice/month Monthly
ROC 2	Immediate Daily Immediate	Weekly 3 times/week Twice a week	Monthly Once a week Weekly	When available Twice/month Monthly
ROC 3	Immediate Daily	Weekly 3 times/week	Monthly Once a week	When available Twice/month
ROC 4	Immediate	Weekly	Monthly	When available

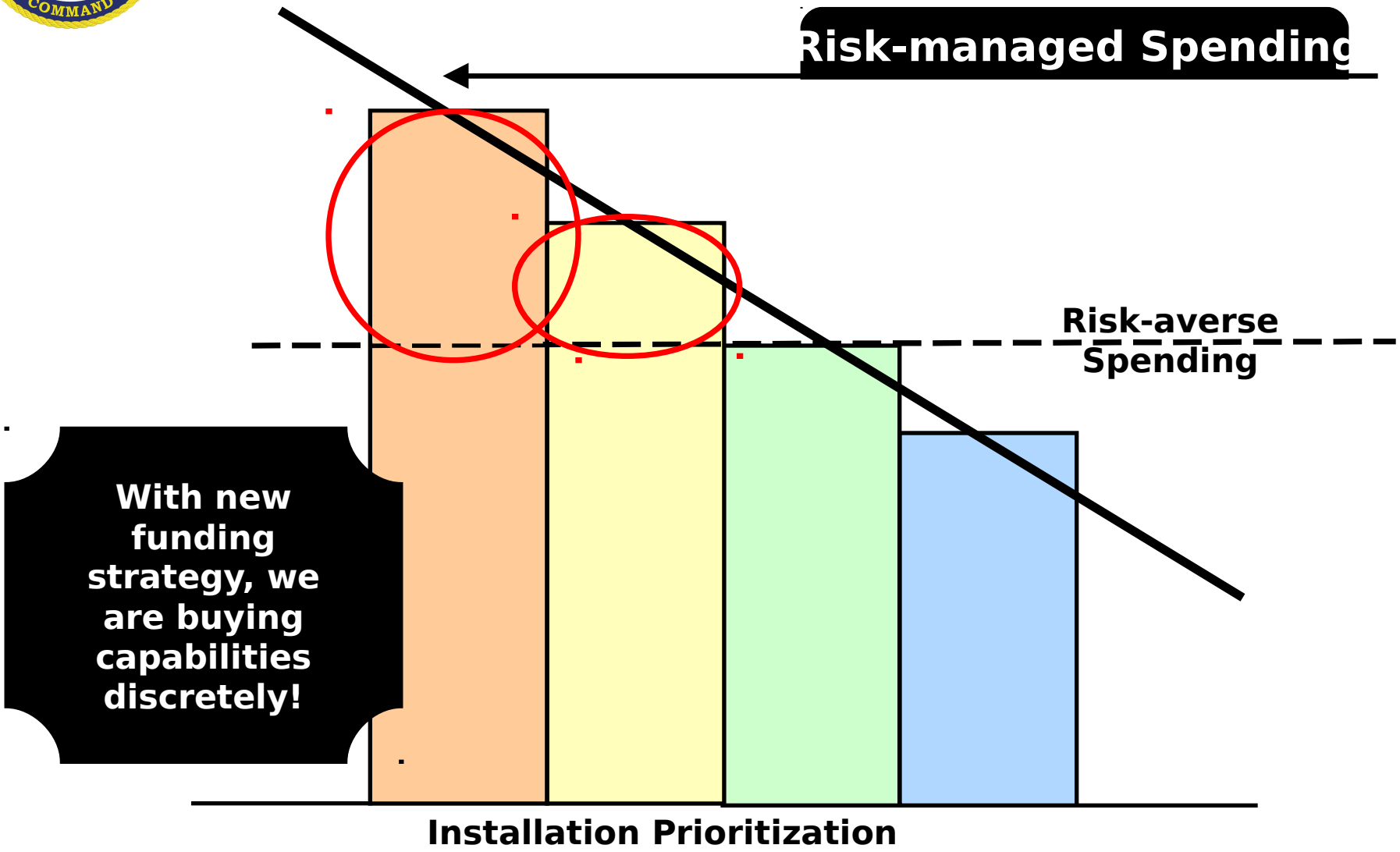
Capability Package (Actual)

Notional Access Control Sample

	CL 1	CL 2	CL 3	CL 4
ROC 1	Immediate Daily KINGS BAY	Weekly 3 times/week Twice a week	Monthly Once a week Weekly	Twice/month Monthly
ROC 2	Immediate	Weekly 3 times/week	KEY WEST MAYPORT	Weekly Twice/month Monthly
ROC 3	Immediate	Weekly Daily	MERIDIAN ATLANTA	When available
ROC 4	 Immediate 3 times/week	Weekly	ATHENS	Weekly Twice/month

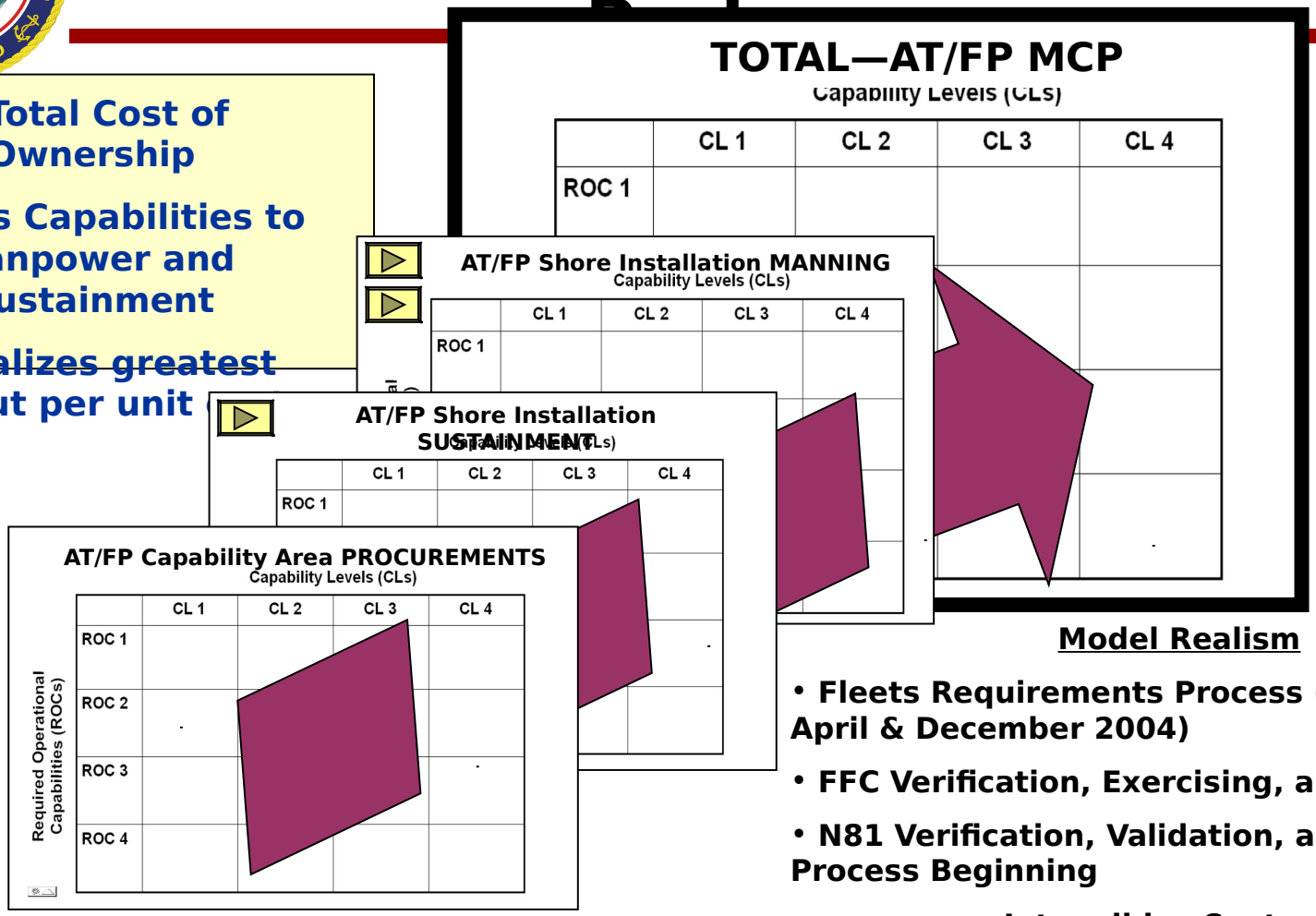

CL 1
CL 2
CL 3
CL 4
ROC 1
ROC 2
ROC 3
ROC 4
KINGS BAY
KEY WEST
MAYPORT
MERIDIAN
ATLANTA
ATHENS

Risk-managed Spending



Ashore AT Capabilities

- **Total Cost of Ownership**
- **Links Capabilities to Manpower and Sustainment**
- **Realizes greatest output per unit**



Model Realism

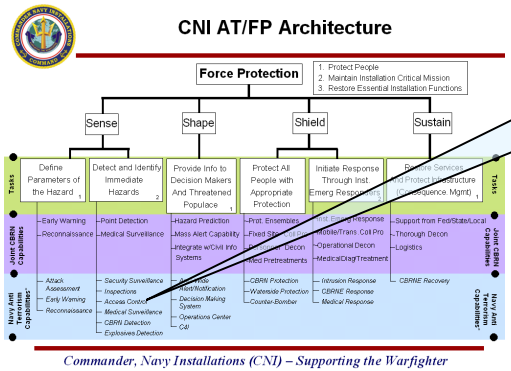
- **Fleets Requirements Process (July 2003, April & December 2004)**
- **FFC Verification, Exercising, and SORTS**
- **N81 Verification, Validation, and Analysis Process Beginning**

Intangibles Captured

- **SAT/SYSCOM Execution Guidance by CNI**

Shore Program Centric Solutions

Moving away from installation centric AT/FP solutions *... to Program Centric AT/FP Solutions.*



Access Control

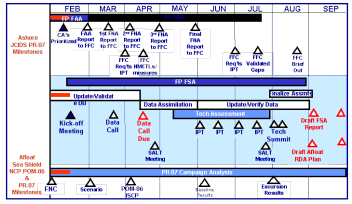
Via CNI w/ SAT

NAVFAC Program Manager

+

N46/CNI Resourcing FYDP

+

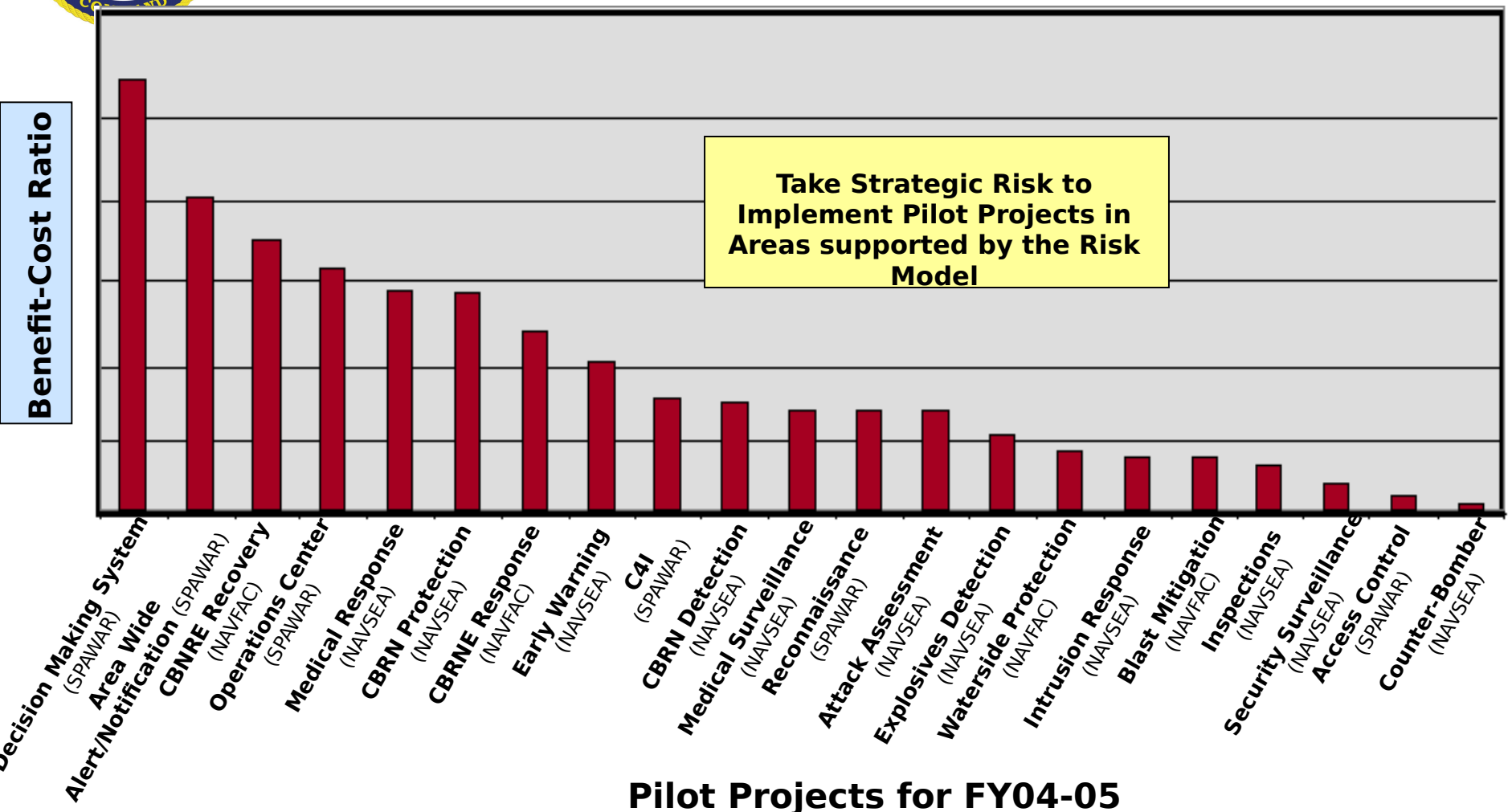


Technology Roadmap (Under Development)

+

FFC IPT Tasks/ (NMETLS)

CNI Risk Based Investment Model



nformation Management & Base Wide Ale | Physical Security/Access Contro

AT/FP Investment in Pilot Programs

	Information Management & Base Wide Alert		Physical Security / Access Control Pilot			
Location	**CNRMA**		**CNRSE**		**CNRSW**	
	Cost	**Date**	**Cost**	**Date**	**Cost**	**Date**
Phase 1 OMN	500,000	February	250,000	January	500,000	February
Phase 2 OMN	1,000,000	August	500,000	August	1,000,000	August
Phase 2 OPN	TBD					
	SPAWAR					

AT/FP Investment in Pilot Programs

Information Management & Base Wide Alert

- CNRMA
- Leave-behind C4I capability (technology and CONOPs) supporting AT/FP and Emergency Management
- Leverage existing technologies
- Evaluate convergence of a solution-set capable of Navy-wide deployment
- Leverage other DoD programs
- Work toward convergence with civil agencies

Physical Security/Access Control

- CNRSE
- Identifying opportunities to reduce required manning/process layering/duplication of effort
  - –Smart Gate technology
  - –Waterside security system
  - –Perimeter intrusion detection system
  - –Perimeter surveillance

Physical Security/Access Control

- CNRSW
- Identifying opportunities to reduce required manning/process layering/duplication of effort
  - Vehicle and personnel access control to piers
  - Enclave personnel tracking
  - Incorporating technology for off-hour manning/monitoring
  - Smart Fence with Sensor back-up
  - Access to North Island

The Way Ahead

From Risk Aversion…

- Cannot afford maximum level of protection everywhere
- “Buying” risk since Khobar Towers, but have not known at what cost

…to Risk Management

- Assigning the right resources to the right place at the right time
- Determining how to distribute resources with respect to the marginal costs of each capability

QUESTIONS?